PRIVACY IMPACT ASSESSMENT

Staffing Systems (Resumix)/Automated Staffing Program

1. **Department of Defense Component:** Defense Logistics Agency.

2. **Name of IT System:** Staffing Systems (Resumix)/Automated Staffing Program (ASP)

3. **Budget System Identification Number (SNAP-IT Initiative Number):** 1832.

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository:** 4283.

5. **IT Investment Unique Identifier (OMB Circular A-11):** N/A.

6. **Privacy Act System of Records Notice Identifier:** OPM-GOVT 5, entitled "Recruiting, Examining, and Placement Records."

7. **OMB Information Collection Requirement Number and Expiration Date:** N/A.

8. **Authority to collect information:**

   Authority as listed in the Privacy notice: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

9. **Brief summary or overview of the IT system:** Resumix/Automated Staffing Program allows the automated collection of resume and applicant information used in the review, referral, and selection of DLA employees through the DLA Merit Promotion Program. The system is owned by the DLA Human Resources. Point of contact is: Ms. Pamela Ries, 614-692-6038, Pam.Ries@dla.mil.

10. **Identifiable Information to be Collected and Nature / Source:** Subject individual's name, SSN, home address, home telephone numbers, and home email address. Source the subject individual (job applicant).

11. **Method of information collection:** Information is collected from the subject individual applicant through the web based Automated Staffing Program (ASP) resume builder and application.

12. **Purpose of the collection:** The records are used in considering individuals who have applied for positions in DLA by making determinations of qualifications, for positions applied for, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion.

13. **Data uses:**

a. To refer applicants, including current and former Federal employees to Federal agencies for consideration for employment, transfer, reassignment, reinstatement, or promotion.

b. To disclose information to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purposes of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision concerning hiring or retaining an employee, issuing a security clearance, conducting a security or suitability investigation of an individual.

c. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

d. By the agency to locate individuals for personnel research or survey response or in producing summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies.

e. To disclose information to the Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of Office rules and rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions; e.g., as prescribed in 5 U.S.C. chapter 12, or as may be authorized by law.

f. To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines or Employee Selection Procedures, or other functions vested in the Commission.

g. To disclose information to the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

14. **Does system derive / create new data about individuals through aggregation?** No.

15. **Internal and External Sharing:**
Internal to DLA: Information is accessed and used by the DLA Human Resources offices and DLA managerial and supervisory personnel making selection decisions.
External to DLA: See information in #13 Data Uses

16. **Opportunities to object to the collection or to consent to the specific uses and how consent is granted:** All personal data collected is voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT system contain a Privacy Act Statement, as required by 5 U.S.C. 552a(b)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the DLA HQ Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection. The subject individual initiates the collection and maintenance of his/her information for the purpose of being considered for employment. Release of this information is done with the individual's full cooperation and consent.

17. **Information provided the individual at Collection, the Format, and the Means of delivery:** A Privacy Act system of records notice was published in the Federal Register with a 30 day public comment period. Forms that collect personal data contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the HQ DLA Privacy Act office during the comment period, during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

18. **Data Controls:**
Administrative: Individual applicant records received through the web based Automated Staffing Program resume builder application are maintained on servers that are located in a controlled secured area with access limited to authorized personnel. Authorized personnel with a need-to-know are granted physical access to computing facilities. Personnel that process sensitive information or unclassified information have been cleared with background investigations and granted approval for access. Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information and are located in 24x7 physically secured locked area,.

Physical: Individual applicant records are maintained in the [redacted] secured area and by authorized personnel that receive initial and Annual Information Assurance training in the operation of Security policies. Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policy. The security policy describe the rules for all applications including Resumix and Automated Staffing Program operations of the DoD information system and clearly delineate user responsibilities and expected behavior of all personnel accessing the website. The rules include the consequences of inconsistent behavior or non-compliance in the DOD Regulation and the Security Rules of Behavior.

Technical: The links to Resumix and Automated Staffing Program applications are located on public web servers accessible to external users. The web based resume and applicant information applications are restricted by the use of the submitter's login and password access. Access is based on the submitter's established passwords [redacted] that verify access to resume and account information. The demilitarized zone is a separate subnet protected by firewall router which further prevents unauthorized access. [redacted] protect the integrity of the application and prevent intrusion. [redacted]

19. **Privacy Act Interface:** OPM-GOVT 5, entitled "Recruiting, Examining, and Placement Records."

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:**
The potential privacy risks regarding the collection, use and sharing of Resumix and Automated Staffing Program information is minimal; information is kept on a protected server protected by [redacted] firewall entrances. Servers where privacy information/records are stored are located in secure facilities that you must have permission to enter. The servers are protected from access [redacted] which deters the risk of access, copying, destruction, and illegal access and distribution of information by unauthorized access.

Threat: Data sharing can occur among authorized personnel with access to the information. All personnel are trained in the process of information handling, annually in the Information Assurance course.

Danger: Dangers in the collection of information can be mitigated by security reviews, guidelines, audit trails and observed in log information which is reviewed by the system administrators.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

21. **Classification and Publication of Privacy Impact Assessment:**
Classification: Unclassified.
Publication: This document will be published either in full or in summary form on the DLA public website, http://www.dla.mil/public_info/efoia/privacy.asp .

DATA OWNER: [redacted] 7/24/08
Name: [redacted] (Signature) (Date)
Title: Human Resource Specialist (Information Systems)
Work Telephone Number: [redacted]
Email: [redacted]

INFORMATION ASSURANCE MANAGER: [redacted] 7/24/08
Name: [redacted] (Signature) (Date)
Title: Information Assurance Manager
Work Telephone Number: [redacted]
Email: [redacted]

CHIEF PRIVACY OFFICER: [redacted] 8/12/08
Name: Lewis Oleinick (Signature) (Date)
Title: Chief Privacy and FOIA Officer
Work Telephone Number: [redacted]
Email: [redacted]

REVIEWING OFFICIAL: [redacted] 16 Sep 2008
Name: Mac De Vincentis (Signature) (Date)
Title: DLA Chief Information Officer
Work Telephone Number: [redacted]
Email: [redacted]